draft-happel-structured-email–trust-00

IETF 119
Status

● Scope: Security and trust considerations for processing structured email
  ○ i.e., mainly addressing any sort of recipient-side MUA!?

● Updates since IETF 118
  ○ None
  ○ Draft update in progress
Status quo

● How is structured email currently processed?

● Large ISPs (Gmail, Yahoo, 1&1, …)
  ○ Manual sender approval / white listing
  ○ Require DKIM/SPF/…

● Open source tools
  ○ KMail and Nextcloud: no restrictions
  ○ Roundcube plugin: reusing “trusted sender” (special address book) feature used for remote images

● M3AAWG BCP forthcoming
Types of security concerns

- Formal representation of data (beyond human-readable text)
  - Privacy issue: data easier to analyze in storage / transit
  - Probably comparable to structured MIME attachments (flight tickets, barcodes)

- Possible divergence between structured and human-readable data
  - Same issue, e.g., exists already for text/plain / text/html inside multipart/alternative

- Automated processing
  - Structured email may afford MUAs to offer automated actions (similar to Sieve filter rules)

- External references
  - Similar to external images referenced in HTML email

- More types?
Mechanisms

- **Content encryption**
  - Full message?
  - Structured data only?

- **Trust**
  - Trusted senders (e.g., address book)
  - Sender signatures (e.g., PGP, SMIME)
  - Domain signatures (e.g., DKIM)
  - Transaction identifiers
Differentiate by use cases?

- “Neutral” structured data
  - E.g., shared news article

- Structured data with personal information
  - E.g., flight reservation
Implementation guidelines

- **Processing structured data**
  - Only if the sender is trusted
  - Otherwise: fall back to text/html or text/plain

- **Inlining data (e.g. images)**
  - Avoids privacy issues on receiver side
Next steps

- Further co-authors?
- Request WG adoption
- Reference implementation
  - Plugin for Roundcube Webmail
  - Currently re-using “trusted sender” (in address book) feature for remote images